

INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE OCCIDENTE

Departamento de Electrónica, Sistemas e Informática
Desarrollo Tecnológico y Generación de Riqueza Sustentable

PROYECTO DE APLICACIÓN PROFESIONAL (PAP)



ITESO, Universidad
Jesuita de Guadalajara

PAP4N01A PROGRAMA DE LA INDUSTRIA DE ALTA TECNOLOGIA I

Bishop Fox

PRESENTA

Alumno: ICS, Salvador Ledezma Pérez

Profesor PAP: Juan Manuel Islas Espinoza, PMP®

Tlaquepaque, Jalisco, Julio 2025.

ÍNDICE

Contenido

| | |
|---|-------------------------------------|
| REPORTE PAP | 3 |
| Presentación Institucional de los Proyectos de Aplicación Profesional | 3 |
| Resumen..... | 4 |
| 1. Introducción | 5 |
| 1.1 Antecedentes | 5 |
| 1.2 Justificación | 5 |
| 1.3 Objetivos | 5 |
| 1.4 Contexto..... | 6 |
| 1.5 Inventario de Competencias | 6 |
| 1.6 Plan Educativo | 7 |
| 1.7 Entregables..... | 7 |
| 1.8 Involucrados..... | 7 |
| 2. Desarrollo del Proyecto PAP..... | 8 |
| 2.1 Administración del Proyecto..... | 8 |
| 2.2 Sustento Teórico y Metodológico | 8 |
| 2.3 Descripción del Proyecto..... | 9 |
| 2.4 Plan de Trabajo | 9 |
| 2.5 Equipo de Trabajo | 10 |
| 2.6 Plan de Comunicaciones | 10 |
| 2.7 Plan de Calidad | 11 |
| 2.8 Seguimiento y Control | 11 |
| 3. Resultados del Trabajo Profesional..... | 12 |
| 3.1 Productos Obtenidos | 12 |
| 3.2 Estimación del Impacto..... | 12 |
| 4. Reflexiones del alumno | 13 |
| 4.1 Aprendizajes Profesionales..... | 13 |
| 4.2 Aprendizajes Sociales..... | Error! Bookmark not defined. |
| 4.3 Aprendizajes Éticos | Error! Bookmark not defined. |
| 4.4 Aprendizajes Personales | Error! Bookmark not defined. |
| 4.5 Tareas Aprendidas..... | Error! Bookmark not defined. |
| 5. Conclusiones..... | 15 |

6. Bibliografía y Anexos (*solo en caso de ser necesarios*).....**Error! Bookmark not defined.**

REPORTE PAP

Presentación Institucional de los Proyectos de Aplicación Profesional

Los Proyectos de Aplicación Profesional (PAP) son una modalidad educativa del ITESO en la que el estudiante aplica sus saberes y competencias socio-profesionales para el desarrollo de un proyecto que plantea soluciones a problemas de entornos reales. Su espíritu está dirigido para que el estudiante ejerza su profesión mediante una perspectiva ética y socialmente responsable.

A través de las actividades realizadas en el PAP, se acreditan el servicio social y la opción terminal. Así, en este reporte se documentan las actividades que tuvieron lugar durante el desarrollo del proyecto, sus incidencias en el entorno, y las reflexiones y aprendizajes profesionales que el estudiante desarrolló en el transcurso de su labor.

Resumen

En este proyecto formo parte del departamento de Cosmos, desempeñando el rol de operador adversario. Mi labor consiste en ejecutar tareas propias de un operador dentro del marco establecido por el proyecto *Cosmos Operations*. Entre mis responsabilidades se encuentran la identificación y explotación de vulnerabilidades en la superficie de ataque de nuestros clientes, la redacción de informes técnicos detallados, el acompañamiento en la mitigación de dichos fallos, la participación en reuniones con los clientes y el desarrollo de herramientas para uso interno del equipo. Con seis años de experiencia en la industria tecnológica, el objetivo de este proyecto es profundizar en habilidades técnicas avanzadas que me permitan especializarme aún más y aportar un valor único dentro del equipo.

1. Introducción

1.1 Antecedentes

Bishop Fox es una empresa reconocida a nivel mundial por su liderazgo en ciberseguridad ofensiva. Se especializa en la realización de pruebas de seguridad sobre una amplia gama de tecnologías, incluyendo aplicaciones móviles, entornos en la nube y plataformas web, entre otras. Ofrece servicios tanto de consultoría como de pruebas de penetración continuas, adaptándose a las necesidades de organizaciones de todos los sectores: desde la industria alimentaria y manufacturera, hasta la médica y financiera, en todo el mundo.

Su misión y valores están alineados con la búsqueda constante de la excelencia. Bishop Fox se propone ser un referente en calidad, investigación y contribución a la comunidad de ciberseguridad. Sus valores reflejan este compromiso, promoviendo la mejora continua tanto a nivel individual como en equipo, así como la creación de un entorno que favorezca ese crecimiento.

1.2 Justificación

El enfoque exclusivo de Bishop Fox en seguridad ofensiva resulta especialmente atractivo para mí, ya que es precisamente el área en la que deseo desarrollarme profesionalmente. La empresa cuenta con un equipo de expertos altamente reconocidos a nivel mundial, con amplia trayectoria en investigación, proyectos relevantes y logros significativos, lo que los convierte en excelentes mentores. Trabajar junto a ellos representa una valiosa oportunidad para continuar creciendo dentro de la industria.

Planeo dedicar las veinte horas del PAP a este proyecto, ya que mi principal objetivo es adquirir experiencia práctica. Si bien ya tengo conocimientos previos en las funciones que desempeñaré, mi intención es perfeccionarlas y consolidar mis habilidades para avanzar dentro del rol.

Durante el proyecto, se me brindarán diversas oportunidades para fortalecer mi aprendizaje: podré hacer shadowing a compañeros con más experiencia, contaré con sesiones semanales con mi mánager para resolver dudas y recibir orientación, y tendré acceso a canales de soporte donde podré aprender directamente del resto del equipo.

1.3 Objetivos

La empresa busca fomentar el desarrollo profesional de nuevos talentos, brindando oportunidades que les permitan avanzar en su carrera mientras completan su formación académica.

En mi caso, me enfocaré en profundizar mis conocimientos en áreas de interés personal, como la explotación de vulnerabilidades en APIs y entornos en la nube. Además, tendré la oportunidad de establecer vínculos con profesionales influyentes en el sector, lo cual contribuirá a mi crecimiento dentro de la industria. También fortaleceré habilidades transversales, especialmente en lo relacionado con la comunicación efectiva en inglés y la interacción con clientes en contextos de trabajo remoto.

1.4 Contexto

Mi participación será como adversarial operator, u operador adversario, dentro del equipo de Cosmos. Este departamento gestiona proyectos individualizados para cada cliente, con una duración estimada de uno a tres años. Cada proyecto se enmarca dentro de un esquema de pruebas de penetración continuas, cuyo propósito es realizar ataques controlados de forma recurrente para detectar vulnerabilidades antes de que puedan ser aprovechadas por agentes maliciosos.

Mi rol operativo dentro de estos proyectos incluirá la identificación y explotación de fallos de seguridad en la infraestructura y superficie de ataque del cliente, la elaboración de reportes técnicos, la comunicación directa con los clientes para resolver dudas o explicar hallazgos, la validación de remediaciones implementadas y el desarrollo de herramientas internas que apoyen al equipo en sus tareas diarias.

1.5 Inventario de Competencias

| No. | Competencia | Req | Adq | GAP | Obj | Prior |
|-----|---|-----|-----|-----|-----|-------|
| 1 | Identificación de exposiciones en la nube | | | | | |
| 1.1 | Exposicion a traves de la API | 3 | | | 4 | 1 |
| 1.2 | Exposicion por politicas vulnerables | 2 | | | 4 | 1 |
| 1.3 | Exposicion por accesos publicos | 2 | | | 4 | 1 |
| 2 | Inglés | | | | | |
| 2.1 | Oral | 5 | | | 5 | 5 |
| 2.2 | Escrito | 5 | | | 5 | 5 |
| 3 | Identificación de vulnerabilidades en APIs | | | | | |
| 3.1 | Enumeración | 4 | | | 4 | 4 |
| 3.2 | Explotación | 4 | | | 4 | 4 |
| 4 | Creación de playbooks | 4 | | | 4 | 4 |
| 5 | Control de calidad | 4 | | | 4 | 5 |
| 6 | Creación de templates | 4 | | | 3 | 5 |
| 7 | Comunicación con clientes | 4 | | | 5 | 4 |
| 8 | Reviews trimestrales a clientes | 4 | | | 5 | 3 |

1.6 Plan Educativo

Plan de Actividades

| No. | Actividad Educativa | Tipo Actividad | Total Hrs | Fecha Inicio | Fecha Terminación | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | Obj | |
|-----|-------------------------------------|----------------|-----------|--------------|-------------------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|-----|--|
| 7 | Comunicación con clientes | Práctica | | | | | | | | | | | | | | | | | | | | | |
| 7.1 | Creación de presentaciones | | | 1/7/2025 | | | | | | | | | | | | | | | | | | | |
| 7.2 | Comunicar la información contenida | | | 1/7/2025 | | | | | | | | | | | | | | | | | | | |
| 2 | Inglés Escrito | Práctica | | | | | | | | | | | | | | | | | | | | | |
| 2.1 | Redacción de reportes | | | 1/6/2025 | | | | | | | | | | | | | | | | | | | |
| 3 | Trabajo en vulnerabilidades de APIs | Autoestudio | | 1/6/2025 | | | | | | | | | | | | | | | | | | | |
| 4 | Creación de playbooks | Práctica | | 1/6/2025 | | | | | | | | | | | | | | | | | | | |
| 6 | Creación de templates | Práctica | | 1/6/2025 | | | | | | | | | | | | | | | | | | | |
| 5 | Control de calidad | Práctica | | 1/6/2025 | | | | | | | | | | | | | | | | | | | |
| 8 | Reviews trimestrales a clientes | Práctica | | 1/7/2025 | | | | | | | | | | | | | | | | | | | |

1.7 Entregables

El producto principal del proyecto será la creación de reportes que documenten las vulnerabilidades encontradas en los sistemas de los clientes. Estos informes se redactarán de manera continua, en función de los descubrimientos realizados durante las actividades diarias. Además, se generarán entregables técnicos complementarios, como documentación especializada y herramientas desarrolladas en código, con el objetivo de apoyar al equipo en sus tareas. Para las reuniones periódicas con los clientes, también se elaborarán presentaciones personalizadas que resuman los hallazgos más relevantes de cada caso.

1.8 Involucrados

- Manager
- Operadores
- Analistas
- Clientes
- Encargados de cuentas de clientes

2. Desarrollo del Proyecto PAP

2.1 Administración del Proyecto

La administración del proyecto se lleva a cabo siguiendo metas definidas por el líder técnico del equipo, junto a los supervisores del equipo de clientes. Durante el inicio del proyecto de cada cliente, se tiene una reunión donde se expresan las metas del proyecto y las reglas a seguir para cada cliente. En la planificación, hay varias juntas que se tienen de forma semanal, con diferentes equipos involucrados; como con el equipo de ingeniería. La ejecución, seguimiento y control, ocurren directamente con el equipo de operadores. Aquí, se nos da una planeación de ejecución semanal, donde se cubren las labores a realizar.

Mis compañeros operadores, dan el seguimiento y control. El seguimiento ocurre en dos juntas semanales y el control ocurre al terminar cada caso. El proceso de control depende del día. Cada día se asigna una persona diferente del equipo a este proceso y se encargan de realizar un control del proceso y verificar los entregables de cada cliente. El cierre es realizado por el líder técnico y los supervisores del equipo de clientes.

2.2 Sustento Teórico y Metodológico

La metodología empleada se basa en un flujo de trabajo interno denominado investigaciones. Este proceso comienza con un analista, quien se encarga de realizar las etapas de rediscovery y triage. A partir de los hallazgos obtenidos en estas fases, se generan casos que posteriormente son asignados a los operadores.

Nuestra labor como operadores consiste en analizar estos casos en profundidad para identificar posibles vulnerabilidades. Una vez concluida la investigación de un caso, elaboramos un documento llamado finding, el cual es entregado al cliente. Este informe detalla la vulnerabilidad descubierta, el método utilizado para explotarla, los impactos asociados y una serie de recomendaciones técnicas orientadas a su remediación.

2.3 Descripción del Proyecto

Mi proyecto se integra directamente en las operaciones comerciales de la organización, específicamente en el rol de Operador Adversarial. Formo parte del equipo de Cosmos, una división de Bishop Fox dedicada a brindar servicios de seguridad ofensiva continua, mediante proyectos de largo plazo para sus clientes. Nuestra misión es ayudarles a detectar vulnerabilidades en sus sistemas antes de que sean explotadas. En este contexto, mis funciones incluyen realizar investigaciones técnicas, documentar hallazgos y comunicarlos formalmente a los clientes, contribuyendo así a las operaciones del equipo.

El flujo de trabajo inicia con el equipo de analistas, que se encarga de mapear y clasificar los activos tecnológicos del cliente. Una vez identificados, estos activos se asignan a los operadores, quienes analizan su seguridad en busca de vulnerabilidades. Tras el análisis, se elabora un informe técnico que se entrega al cliente como primer producto del proceso. Además, cada trimestre se realiza una reunión de seguimiento —el segundo entregable— en la que se presentan los resultados obtenidos y se aclaran dudas.

Entre las herramientas tecnológicas esenciales para generar estos entregables se encuentran:

- La plataforma interna de Cosmos
- GitHub, para la colaboración y gestión de herramientas
- AWS, como infraestructura base para análisis y despliegue

2.4 Plan de Trabajo

| Actividad | SEMANA 1 | SEMANA 2 | SEMANA 3 | SEMANA 4 | SEMANA 5 | SEMANA 6 | SEMANA 7 |
|------------------------|-----------------|----------|----------|----------|----------------|----------|----------|
| Proyecto PAP | [Barra naranja] | | | | | | |
| Investigaciones | [Barra verde] | | | | | | |
| Redacción de Reportes | [Barra azul] | | | | | | |
| Reuniones con Clientes | | | | | [Barra morada] | | |

2.5 Equipo de Trabajo

| <i>Rol</i> | <i>Responsabilidad</i> | <i>Nombre (opcional)</i> |
|------------------------|---|--------------------------|
| Líder Técnico | <p>Establecer planes de trabajo para el equipo</p> <p>Resolver problemas técnicos o de procesos</p> <p>Mantener la comunicación entre todas las demás partes del equipo</p> | |
| Operador (Alumno) | <p>Realizar investigaciones en los activos de los clientes</p> <p>Comunicar vulnerabilidades</p> <p>Resolver dudas de clientes respecto a los reportes</p> | |
| Analista | <p>Identificar los activos de los clientes</p> <p>Comunicar hallazgos</p> <p>Resolver dudas del equipo y los clientes sobre la plataforma</p> | |
| Supervisor de clientes | <p>Mantener la comunicación con los clientes</p> <p>Comunicar las necesidades de los clientes con el resto del equipo</p> <p>Resolver conflictos con los clientes</p> | |

2.6 Plan de Comunicaciones

| <i>Emisor</i> | <i>Mensaje</i> | <i>Receptor</i> | <i>Medio</i> | <i>Frecuencia</i> |
|---------------|-----------------|-----------------|---------------|-------------------|
| Alumno | Dudas y avances | Profesor PAP | Video llamada | Mensual |

| | | | | |
|---------------|---------------|----------|--------------------------------------|--------|
| Alumno | Reportes | Clientes | Archivo electrónico y video llamadas | Diario |
| Líder técnico | Planificación | Equipos | Video llamadas | Diario |

2.7 Plan de Calidad

| Emisor: <i>Quién Entrega</i> | Entregable: <i>Qué Entrega (SubEntregable)</i> | Receptor: <i>Quién recibe o Inspecciona</i> | Criterios: <i>Condiciones de Aceptación</i> | Siguiente paso. <i>Donde va Cuando se Autoriza.</i> |
|--|--|---|---|---|
| Operador a cargo de investigación | Reporte | Operador en turno | Lineamientos de reportes de Operadores | Plataforma de Cosmos |
| Operador (Alumno) | Presentación Powerpoint | Líder Técnico | Guía de estilo de Cosmos | Reunión con el cliente |

2.8 Seguimiento y Control

El seguimiento del proyecto se realiza mediante una reunión semanal cada viernes, en la que se evalúa el avance, se aplican ajustes necesarios y se intercambia retroalimentación entre ambas partes. Estas sesiones son fundamentales para alinear expectativas, realizar correcciones a tiempo y asegurar que mis metas dentro del proyecto se mantengan en foco y sean consideradas.

Paralelamente, en el marco del proyecto PAP, asisto a clases semanales con mi profesor, lo cual me brinda un espacio para resolver dudas, recibir orientación y obtener retroalimentación constante. Además, se llevan a cabo reuniones mensuales en las que se revisa mi progreso de manera formal y se proporcionan observaciones directas sobre el desarrollo de mi reporte.

3. Resultados del Trabajo Profesional

3.1 Productos Obtenidos

- Hallazgos: Documentos que describen el procedimiento utilizado para detectar, aprovechar y evaluar la severidad de una falla de seguridad.
- Informes para clientes: Exposiciones que resumen los avances recientes, patrones observados y estrategias de mejora implementadas durante el último trimestre.

3.2 Estimación del Impacto

La relevancia de los entregables y mi contribución ha sido significativa. Las investigaciones que llevé a cabo se enfocaron en entornos reales y activos pertenecientes a clientes. Cada vulnerabilidad detectada representaba una amenaza legítima, susceptible de ser aprovechada por atacantes con intenciones maliciosas, lo que podría haber resultado en accesos no autorizados a datos sensibles, pérdida de información, o interrupciones críticas en servicios operativos, entre otros posibles escenarios de alto riesgo.

4. Reflexiones del alumno

4.1 Aprendizajes Profesionales

Uno de los aprendizajes más importantes a nivel profesional fue comprender cómo opera el sector. Entender las prioridades y necesidades particulares de cada organización resultó esencial para ayudarlas a proteger sus activos críticos de forma eficaz. Asimismo, fortalecí mis habilidades de comunicación en inglés, tanto en su vertiente escrita como oral. Esto fue clave para traducir hallazgos técnicos a un lenguaje comprensible para audiencias no especializadas, y al mismo tiempo, comunicarme con claridad con los equipos técnicos responsables de mitigar los riesgos. Estas competencias también facilitaron una interacción fluida con mis compañeros de equipo.

4.2 Aprendizajes Sociales

El impacto social más relevante se refleja en la protección de la información personal y los servicios esenciales que las personas utilizan a diario. Al colaborar con empresas del sector salud y financiero, comprendí la responsabilidad que implica trabajar con datos delicados y sistemas que, en caso de fallar, podrían generar consecuencias serias. También recibí respaldo para impulsar proyectos propios, los cuales me permitieron fomentar la educación y concientización sobre ciberseguridad a nivel regional.

4.3 Aprendizajes Éticos

El componente ético es central en esta profesión. Al contar con altos niveles de acceso y confianza por parte de los clientes, se vuelve indispensable manejar esos privilegios con responsabilidad. Aprendí la importancia de ceñirme estrictamente a los permisos acordados para cada prueba, evitando cualquier tipo de abuso de acceso o visualización de datos no autorizados, incluso si era técnicamente posible.

Mantener la confidencialidad de la información sensible fue otra lección clave. La ética profesional exige no solo cumplir normas, sino actuar con integridad, usar las herramientas de manera responsable y mantener un compromiso constante con la transparencia y el respeto hacia los derechos y la privacidad de los usuarios.

4.4 Aprendizajes Personales

Esta experiencia me ofreció una visión concreta de cómo funciona la industria y qué esperan realmente las empresas. Descubrí la relevancia de las habilidades interpersonales, como saber comunicarse, colaborar en equipo y presentar resultados de manera comprensible para diferentes públicos. Estas destrezas resultan esenciales para complementar el conocimiento técnico y aportar valor al equipo.

También logré entender todo el trabajo invisible que se realiza para resguardar la información digital. Valorar estos esfuerzos me permitió confirmar mi deseo de continuar mi desarrollo profesional en el ámbito de la ciberseguridad. Gracias a la guía de mis mentores y colegas, me sentí motivado a desarrollar iniciativas propias y a superar desafíos complejos, descubriendo así mis fortalezas.

4.5 Tareas Aprendidas

El éxito de mi participación en el proyecto PAP se debió en gran parte a la buena planificación y al uso de estrategias efectivas. La gestión adecuada del tiempo fue crucial, lo que logré mediante calendarios y asignación precisa de tareas, permitiéndome equilibrar responsabilidades académicas y laborales. La colaboración continua con el equipo y una comunicación clara facilitaron la resolución de obstáculos tanto técnicos como organizativos.

Además, identificar personas clave y recursos que ofrecieran guía marcó una gran diferencia. Mis mentores no solo compartieron conocimientos, sino que también me ayudaron a superar barreras y seguir creciendo. Finalmente, aprendí el valor de crear documentación propia, como manuales, procesos y aprendizajes, que facilitaron la continuidad del trabajo y fortalecieron mi comprensión general del proyecto.

5. Conclusiones

El desarrollo del proyecto PAP representó una experiencia profundamente formativa y satisfactoria, que dejó aprendizajes valiosos tanto en el ámbito profesional como en el personal. Me permitió adentrarme de manera práctica en el sector de la ciberseguridad, comprendiendo las demandas del entorno y las competencias necesarias para ejercer con profesionalismo. Esta inmersión me ayudó a dimensionar la complejidad y el esfuerzo que hay detrás de las medidas que protegen la información de usuarios y organizaciones, fortaleciendo así mi convicción de continuar una carrera en esta área.

Además, la experiencia fue un catalizador para mi crecimiento personal, permitiéndome identificar y desarrollar mis capacidades para enfrentar desafíos técnicos y organizativos. Tuve la oportunidad de colaborar con referentes de la industria, así como de avanzar en proyectos propios enfocados tanto en aspectos técnicos como en iniciativas de divulgación y construcción de comunidad.

Desde una perspectiva ética, interioricé la importancia de gestionar con responsabilidad los accesos privilegiados y la información sensible, así como de aplicar prácticas que garanticen el cumplimiento estricto de los límites definidos para cada actividad. En el terreno técnico, exploré distintas áreas del sector y comencé a especializarme en temas de interés como la seguridad en APIs y entornos en la nube.

El logro de los objetivos del proyecto fue posible gracias a la aplicación de elementos estratégicos clave: una planificación rigurosa, una buena administración del tiempo, una comunicación clara dentro del equipo, el aprovechamiento de recursos y personas de apoyo, y la elaboración de documentación detallada que facilitó la continuidad y el aprendizaje compartido. Estos factores favorecieron una ejecución ordenada y eficiente.

Uno de los principales retos fue mantener el equilibrio entre las exigencias académicas y las del proyecto. Si bien la experiencia fue enriquecedora, coordinar ambos compromisos resultó desafiante debido a la rigidez de los calendarios escolares. En ocasiones, cumplir con los plazos representó una dificultad significativa. No obstante, haber superado este reto me deja una gran satisfacción y demuestra mi capacidad para perseverar ante escenarios complejos.